Problem (ne)odlučivosti

Marić, Lucija

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Lucija Marić

PROBLEM (NE)ODLUčIVOSTI

Diplomski rad

Voditelj rada:
doc. dr. sc. Franka Miriam Brückler

Zagreb, rujan, 2022.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Ovaj rad posvećujem svojim roditeljima.
Majci, koja me uvijek gura i bez koje ovo ne bi bilo moguće.
Ocu, mom anđelu čuvaru, koji mi je najveća motivacija.
Hvala bratu Frani i dragim prijateljima na podršci.
Hvala mentorici doc. dr. sc. Franki Miriam Brückler na neizmjernom strpljenju i izvrsnom vodstvu u pisanju rada.

Moramo znati – znat ćemo!

Sadržaj

Sadržaj **iv**

Uvod **1**

1 Povijest problema (ne)odlučivosti **3**

2 Primjeri neodlučivih problema **17**
2.1 Igra života 17
2.2 Wangove pločice 22
2.3 Hilbertov deseti problem 26
2.4 *Magic: The Gathering* 29

3 Zaključak **31**

Bibliografija **33**

Uvod

Uvijek će postojati istinite tvrdnje koje neće biti moguće dokazati. To otkriće transformiralo je pojam beskonačnosti, promijenilo tok Drugog svjetskog rata i dovelo do izuma modernog računala. Naime, pokušavajući riješiti problem (ne)odlučivosti, Alan Turing napravio je Turingov stroj koji je osnova svakog računala i mobilnog telefona. Problem (ne)odlučivosti sastoji se u traženju odgovora na pitanje: Postoji li efektivna metoda (algoritam) kojom bi se za danu matematičku tvrdnju moglo ustanoviti je li istinita ili nije (u svim logičkim strukturama danog aksiomatskog sustava)? Taj problem dio je Hilbertovog programa, programa istraživanja temelja matematike kojeg je 1920ih godina postavio njemački matematičar D. Hilbert. Hilbert je bio uvjeren da je odgovor na njega pozitivan. Međutim, pitanje je negativno riješeno rezultatima K. Gödela i A. Turinga.

U ovom radu inspiriranom videom [25] opisat ćemo povijest problema (ne)odlučivosti i osvrnuti se na uloge znamenitih matematičara i logičara poput Cantora, Russella, Hilberta, Gödela i Turinga. U drugom dijelu predstaviti primjere dokazano neodlučivih problema kao što su Conwayeva igra života i problem Wangovih pločica.

Poglavlje 1

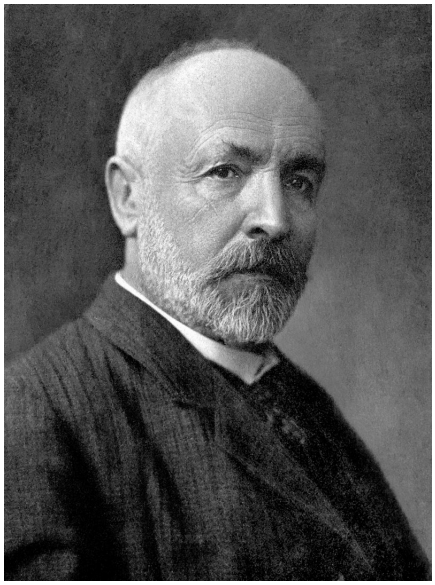
Povijest problema (ne)odlučivosti

1874. godine njemački matematičar Georg Cantor (1845.–1918., slika 1.1) objavio je članak *Über eine Eigenschaft des Inbegriffs aller reellen algebraischen Zahlen* kojim je pokrenuo novu granu matematike – teoriju skupova. Rođen je u St. Petersburgu, ali s obitelji je odselio u Njemačku kad je imao 11 godina. Od 1890ih počeo je pokazivati vrlo ekscentrično ponašanje i patiti od napada depresije te je umro u sanatoriju. Studirao je matematiku u Zürichu i Berlinu, a 1867. godine doktorirao je s temom iz teorije brojeva. Za matematičku analizu zainteresirao ga je Eduard Heine (1821.–1881.) sa sveučilišta u Halleu. Heine mu je zadao zadatak da proučava uvjete jedinstvenosti reprezentacije funkcije svojim Fourierovim redom . Razmatrajući razne uvjete na domenu funkcije, počeo je razmatrati precizniji opis linearnog kontinuuma realnih brojeva. Godine 1870. definirao je realne brojeve kao klase ekvivalencije Cauchyjevih nizova racionalnih brojeva i dokazao bijekciju skupa realnih brojeva s točkama pravca (tj. dokazao je da realni brojevi čine kontinuum). To je dovelo do toga da se Cantor počeo više posvećivati skupu realnih brojeva $\mathbb{R}$ i općenito beskonačnim skupovima. 1873. godine dokazao je ekvipotentnost (jednakobrojnost) skupova $\mathbb{N}$ i $\mathbb{Z}$ koristeći kao definiciju da su dva skupa ekvipotentna[1] ako postoji bijekcija s jednoga na drugi. Skupovi ekvipotentni s $\mathbb{N}$ nazivaju se prebrojivim skupovima, a njihov kardinalni broj označava se s $\aleph_0$. Iste godine dokazao je i prebrojivost skupa racionalnih brojeva $\mathbb{Q}$, te skupa svih algebarskih brojeva[2]. Zanimalo ga je jesu li možda svi beskonačni skupovi prebrojivi, ali u već spomenutom članku iz 1874. godine, dao je odgovor da nisu, tj. da postoje beskonačni skupovi s različitim brojevima elemenata. Naime, dokazao je da skup realnih brojeva $\mathbb{R}$ nije ekvipotentan sa skupom prirodnih brojeva $\mathbb{N}$, tj. da je $\mathbb{R}$ neprebrojiv.

Nešto kasnije, 1877. godine, Cantor je, između ostalog, precizirao pojam ekvipotent-

[1] Skupovi su ekvipotentni ako imaju jednako mnogo elemenata.

[2] Algebarski brojevi su oni realni brojevi koji su rješenja polinomijalnih jednadžbi s cjelobrojnim koeficijentima.



Slika 1.1: Georg Cantor (*public domain* slika preuzeta s Wikipedije)

nosti, uveo oznaku $\sim$ za ekvipotentnost i dokazao da su prebrojivi skupovi najmanji beskonačni skupovi. Prema tome, kardinalni broj skupa $\mathbb{N}$, $\aleph_0$ je najmanji beskonačni kardinalni broj, a prema članku iz 1874. godine, on je manji[3] od kardinalnog broja skupa $\mathbb{R}$ (koji se označava s $\mathfrak{c}$):

$$\aleph_0 < \mathfrak{c}.$$

Cantor je postavio **hipotezu kontinuuma** da ne postoji kardinalni broj između ta dva, tj. da je najmanji kardinalni broj veći od $\aleph_0$, u oznaci $\aleph_1$, jednak $\mathfrak{c}$. Budući da je uspio dokazati da je $\mathfrak{c} = 2^{\aleph_0}$, hipoteza kontinuuma obično se zapisuje formulom:

$$2^{\aleph_0} = \aleph_1.$$

No, svi Cantorovi pokušaji dokaza te hipoteze bili su neuspješni i smatra se da je njegova kasnija depresija dijelom potaknuta tim neuspjesima. S druge strane, 1890ih godina dokazao je tzv. osnovni Cantorov teorem teorije skupova (svaki skup ima manje elemenata nego njegov partitivni skup). Trivijalna posljedica tog teorema je da od svake beskonačnosti postoji veća, odnosno da postoji beskonačno mnogo različitih beskonačnosti. Sam Cantor nije bio uznemiren prividnom kontradikcijom između teorema da uvijek postoji još jedna beskonačnost veća od dane druge beskonačnosti i evidentne činjenice da se ne može prekoračiti „apsolutna beskonačnost“ koja se sastoji od svih beskonačnosti. Za duboko religioznog Cantora, to je bilo ne samo matematički smisleno, nego je imalo i jasno teološko

[3] Kardinalni broj a skupa A je manji ili jednak kardinalnom broju b skupa B ako postoji injekcija s A u B. Kardinalni broj a je manji od b ako je manji ili jednak, a nisu jednaki.

tumačenje, ali mnogi drugi nisu dijelili njegov pogled. Tako je Cantorova teorija skupova izazvala gnjev brojnih matematičara toga doba i pokrenula „krizu“ u samim temeljima matematike.[25, 5]

Naime, još od Euklidovih elemenata bilo je opće prihvaćeno kako se provode geometrijski dokazi i da se svi teoremi moraju moći svesti na aksiome. U „Elementima”[4] je Euklid pristupio izgradnji geometrije kao deduktivne znanosti pa stoga treba najprije odrediti temeljne pojmove koji se ne dokazuju (definicije, aksiomi i postulati),[5] a onda pomoću njih dokazati ostale tvrdnje[5]. Euklidovih pet aksioma glasi:

1. Dvije stvari koje su jednake trećoj su i međusobno su jednake.[6]
2. Ako jednakom dodamo jednako, dobit ćemo jednako.
3. Ako jednakom oduzmemo jednako, dobit ćemo jednako.
4. Ono što se podudara je jednako.
5. Cjelina je veća od dijela.

Zatim slijedi Euklidovih pet postulata:

1. Od jedne točke k drugoj povući dužinu.
2. Proizvoljno produljiti dužinu.
3. Oko proizvoljne točke nacrtati kružnicu proizvoljnog promjera.
4. Svi pravi kutevi[7] su jednaki.
5. Ako pravac siječe dva pravca tako da je zbroj unutrašnjih kuteva s iste strane manji od dva prava kuta, onda se ta dva pravca (ako se dovoljno produže) na toj strani sijeku.

Pomoću ovih aksioma dokazivale su se sve daljnje propozicije. Npr. 4. propozicija iz Euklidovih „Elemenata” glasi[19]:

[4]Euklidovi „Elementi” su prvo sustavno deduktnivno matematičko djelo s aksiomatksim pristupom. Napisani su oko 300. g. pr. Kr. i do 20. stoljeća ostali su uzor matematičkog teksta.

[5]Kod Euklida razlika aksioma i postulata je da su postulati isključivo geometrijske tvrdnje, dok se aksiomi odnose i na prirodne brojeve i na geometrijske objekte.

[6]Kod geometrijskih objekata pod jednakošću Euklid podrazumijeva jednakost mjere (duljine, površine, volumena).

[7]Euklid pravi kut definira ovako: Ako pravac upada na drugi pravac čineći susjedne kuteve jednakima, svaki od ta dva prava kuta je pravi.

Propozicija 1. *Ako su dana dva trokuta takva da su dvije stranice jednog jednake dvjema odgovarajućim stranicama drugog i ako su kutovi između tih stranica jednaki, onda su ti trokuti sukladni.*[8]

Dokaz. Neka su ABC i DEF trokuti i vrijedi $|AB| = |DE|$, $|AC| = |DF|$, te $\angle BAC = \angle EDF$. Ako trokut ABC postavimo na trokut DEF tako da je točka A postavljena na točku D, a stranica $\overline{AB}$ na stranicu $\overline{DE}$, tada se i točka B podudara s točkom E jer je $|AB| = |DE|$. Također stranica $\overline{AC}$ podudara se sa stranicom $\overline{DF}$ jer je $\angle BAC = \angle EDF$. Stoga, točka C se podudara s točkom F jer $|AC| = |DF|$. Sada vidimo da se i stranica $\overline{BC}$ podudara sa stranicom $\overline{EF}$, tj. po 4. aksiomu jednake su stranice $\overline{BC}$ i $\overline{EF}$. Stoga se i cijeli trokut ABC podudara s trokutom DEF pa opet prema 4. aksiomu slijedi da su ti trokuti međusobno jednaki. Preostali kutevi također se podudaraju pa su, ponovno prema 4. aksiomu, jednaki. Suvremeno rečeno, budući da su svi elementi ta dva trokuta jednaki, oni su sukladni. □

Ovaj princip dokazivanja bio je uzor stoljećima, ali tek krajem 19. stoljeća počinju se aksiomatizirati i druge matematičke discipline. Npr. talijanski matematičar Guiseppe Peano (1858.–1932.) je u svom djelu *Arithmetices principia nova methodo exposita* 1889. godine predstavio skup aksioma kojim se nadao da će jasno precizirati aritmetiku. Poput mnogih suvremenih matematičara, smatrao je da je matematika savršena i da se to može pokazati jasnim formuliranjem aksioma i dokaza, što bi ujedno bilo i dovoljno da se izbjegnu pogreške i olakša njen razvoj. U originalnoj verziji *Arithmetices principie* predstavio je devet aksioma. Pet od njih je kasnije modificirano i predstavljeno kao **Peanovi aksiomi aritmetike**:[9]

1. Broj nula, 0, je prirodan broj: $0 \in \mathbb{N}$.[10]
2. Sljedbenik[11] svakog prirodnog broja je prirodni broj: $n + 1 \in \mathbb{N}\ \forall n \in \mathbb{N}$.
3. Nikoja dva različita broja nemaju istog sljedbenika: $n + 1 = m + 1 \Rightarrow n = m\ \forall m, n \in \mathbb{N}$.
4. Nula nije sljedbenik nijednog broja: $0 \neq n + 1\ \forall n \in \mathbb{N}$.
5. Ako 0 ima neko svojstvo i ako za svaki prirodan broj koji ima to svojstvo njegov sljedbenik također ima to svojstvo, onda svaki prirodan broj ima to svojstvo: $M \subseteq \mathbb{N}\ \&\ 0 \in M\ \&\ \forall n(n \in M \Rightarrow n + 1 \in M) \Rightarrow M = \mathbb{N}$.

[8] Euklid kaže: onda im je jednaka i treća stranica, trokuti su jednaki i preostali kutovi, tj. oni nasuprot jednakih stranica, su jednaki.

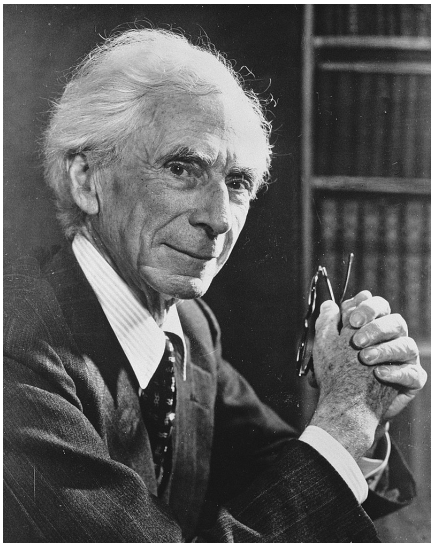
[9] Pod aritmetikom misli se, u antičkoj tradiciji, na teoriju brojeva u skupu $\mathbb{N}$. Antički Grci su samo prirodne brojeve smatrali brojevima, tako da se Peanovi aksiomi ponekad navode bez isticanja pridjeva „prirodni".

[10] U izvornoj verziji: Broj 1 je prirodan broj.

[11] Sljedbenik broja n je definiran kao broj za 1 veći od n, u oznaci $n + 1$.

Nakon što je formulirao osnovne aksiome aritmetike, Peano je pokušao formulirati i osnovne aksiome geometrije i logike. Tada se činilo da je aksiomatizacijom matematika postala dobro utemeljena, s jasnim „pravilima igre". Vjerovalo se da se svi teoremi neke discipline mogu izvesti iz prikladno odabranih aksioma, no (ne samo) uslijed pojave teorije skupova došlo je do rasprave o tome koja sredstva su dozvoljena u matematičkim dokazima [29].

Za raspravu o smislu i matematičkoj korektnosti teorije skupova posebno bitnima su se pokazali paradoksi otkriveni na prijelazu 19. u 20. stoljeće, koji proizlaze iz Cantorove „naivne" (neaksiomatizirane) teorije skupova. Među njima je najpoznatiji **Russellov paradoks**, nazvan po engleskom logičaru Bertrandu Russellu (1872.–1970., slika 1.2). Russellov paradoks obično se popularno opisuje kao paradoks brijača: Zamislimo da neki brijač brije one i samo one muškarce koji sami sebe ne briju. Brije li taj brijač sam sebe ili ne? Ako se brije, značilo bi da se ne brije i obrnuto, ako sam sebe ne brije, morao bi se brijati. Russell je ovaj paradoks objavio u knjizi *The Principles of Mathematics* 1903. godine, a možemo ga opisati i u terminima skupova. Russell je naime primijetio da skup svih skupova koji ne sadrže sami sebe, tj. skup X definiran s $X = \{A : A \notin A\}$ dovodi do kontradikcije na isti način kao i primjer s brijačima: Je li i tako definiran skup X i sam element skupa X?



Slika 1.2: Bertrand Russell (*public domain* slika preuzeta s Wikipedije)

Na jednoj strani rasprave o temeljima matematike bili su **intuicionisti** predvođeni nizozemskim matematičarom L. E. J. Brouwerom i njemačkim matematičarom H. Weylom. Prema intuicionistima, dopušteni su samo tzv. konstruktivni dokazi, u kojima se tvrdnja

dokazuje (ili opovrgava) direktnom konstrukcijom. Oni su smatrali da je Cantorov rad besmislica i da beskonačnosti zapravo ne postoje jer filozofija matematike ne treba samo dosljednost i dokaze, već i intuicije kojima bi se opravdalo postojanje matematičkih objekata. Znameniti francuski matematičar Henri Poincaré (1854.–1912.) je primjerice izjavio: „Kasniji naraštaji smatrat će teoriju skupova bolešću od koje smo se oporavili". Intuicionisti često imaju zajednički pogled s konstruktivistima koji smatraju da matematički objekt postoji samo onda kada se može konstruirati, tj. dokazi egzistencije objekata s nekim svojstvom su prihvatljivi samo ako daju eksplicitnu konstrukciju jednog takvog objekta. Leopold Kroenecker (1823.–1891), jedan od glavnih predstavnika konstruktivista i urednik časopisa u kojem je Cantor objavio svoje prve (vrlo nekonstruktivističke) dokaze iz teorije skupova, smatra se predintuicionistom, te je u spomenutoj debati nazvao Cantora „znanstvenim šarlatanom" i „onim koji korumpira mlade".

S druge strane bili su **formalisti**, koji su podržavali klasični pristup u kom se svi teoremi prema danim pravilima mogu svesti na aksiome. Oni su smatrali da se matematika može staviti na čvrste logičke temelje pomoću Cantorove teorije skupova. Formalizam pokušava reducirati matematičke probleme na formalne izjave i potom dokazati da su rezultirajući formalni aksiomatski sustavi potpuni[12] i konzistentni.[13]. Njihov neformalni vođa bio je veliki njemački matematičar David Hilbert (1862.–1943., slika 1.3). On je bio prvi koji je upotrijebio izraz „formalizam" iako u početku nije imao namjeru upućivati na filozofsko stajalište. Hilbert je izjavio: "Iz raja kojeg nam je stvorio Cantor neće nas nitko moći istjerati" [25, 5, 4, 22].

Intuicionisti su se radovali Russellovom i drugim paradoksima (Cantorovom, Burali-Fortijevom) teorije skupova jer su mislili da je dokazao da je njima teorija skupova opovrgnuta; čak su predložili radikalne mjere koje bi zabranile ne samo Cantorove beskonačnosti već i brojne druge metode. No, to nije bilo tako jednostavno jer su rezultati teorije skupova u to doba već imali bitnih posljedica u drugim granama matematike, primjerice teorija skupova postala je temelj teorije mjere. Stoga su formalisti našli rješenje za sprečavanje skupovnoteoretskih paradoksa u aksiomatizaciji teorije skupova, koja je dovršena 1922. u obliku tzv. Zermelo-Fraenkelovog sustava aksioma teorije skupova. Formalizam koji je početkom 20. stoljeća doveo ne samo do aksiomatizacije teorije skupova, već i drugih disciplina, štoviše i nove aksiomatizacije euklidske geometrije, proizašao je iz tzv. Hilbertove škole [25, 2].

David Hilbert bio je njemački matematičar i jedan od najistaknutijih matematičara toga doba. Rođen je u Königsbergu (današnjem Kalinjingradu), gdje je i odrastao. Doktorirao je na Königsberškom Sveučilištu te tamo ostao raditi kao profesor. Kasnije se zaposlio

[12] Aksiomatski sustav je potpun kada se za svaku tvrdnju može iz tih aksioma dokazati je li istinita ili lažna.

[13] Aksiomatski sustav je konzistentan ako ne sadrži kontradikciju, tj. ne postoji tvrdnja za koju bi se iz tog sustava moglo izvesti da je i istinita i lažna.

Slika 1.3: David Hilbert (*public domain* slika preuzeta s Wikipedije)

na Sveučilištu u Göttingenu gdje je radio do kraja svoje karijere, dok nacisti nisu zabranili Židovima da predaju. Djelovao je na različitim područjima i dao velike doprinose u područjima algebre, teorije brojeva, geometrije, analize i logike. 1900. godine održao je znamenit govor na 2. svjetskom matematičkom kongresu u Parizu. Naslov njegovog predavanja bilo je jednostavno *Matematički problemi* i u njemu je izrazio svoje uvjerenje o rješivosti svih matematičkih problema; čak je to proglasio aksiomom. Predavanje je započeo znamenitim riječima, ovdje u slobodnom prijevodu [11]: „Tko od nas ne bi rado podigao veo ispod kojeg se skriva budućnost, da baci pogled na predstojeće napretke naše znanosti i tajne njezina razvoja tijekom nadolazećih stoljeća! Koji će posebni ciljevi kojima će težiti vodeći matematički umovi budućih generacija? Koje nove metode i nove činjenice će otkriti nova stoljeća — na širokom i bogatom polju matematičkog razmišljanja?". Tom je prigodom istaknuo i tada neriješene matematičke probleme koje je smatrao fundamentalnima za daljnji razvolj matematike. Tu početnu listu od deset problema u sljedeće je dvije godine dopunio do znamenitog popisa 23 Hilbertova problema. Prvi Hilbertov problem je bio upravo spomenuta Cantorova hipoteza kontinuuma, a drugi dokaz da je sustav aksioma aritmetike konzistentan.

U spomenutom je govoru Hilbert predložio da se u aksiomatskom pristupu bilo kojoj matematičkoj disciplini potrebno dokazati nezavisnost[14], potpunost i konzistentnost pojedinog sustava aksioma. Bilo je jasno da Hilbert smatra da se svaki matematički problem može riješiti, samo je ponekad potrebno dosta vremena. Stoga, početkom 1920.–ih godina,

[14] Aksiom u nekom aksiomatskom sustavu je nezavisan od ostalih ako se ne može dokazati (ni opovrgnuti) iz ostalih aksioma tog sustava.

Hilbert iznosi novi prijedlog za utemeljenje i ujedinjenje matematike koji je postao poznat kao **Hilbertov program**. Radi se o pokušaju ujedinjenja različitih tada još novih rezultata: teorije skupova, logičke algebre, ali i klasičnih aksiomatiziranih matematičkih disciplina (aritmetike i geometrije). Poziva se na formalizaciju čitave matematike u aksiomatskom obliku, zajedno s dokazom da je takva aksiomatizacija dosljedna. Sam dokaz dosljednosti trebao je biti izveden koristeći isključivo ono što je Hilbert nazivao *konačnim* metodama. Među ostalim, u Hilbertovom programu i sami dokazi postaju predmet (a ne samo metoda) proučavanja matematike. Malo preciznije, Hilbertov program sastoji se od dva zahtjeva [13]:

1. „Sve, što dosad čini bit matematike, odsad se strogo formalizira, tako da prava matematika ili matematika u užem smislu postaje inventar dokazivih formula."

2. „K toj pravoj matematici dolazi jedna u nekom smislu nova matematika, metamatematika, koja služi osiguranju prve. [...] U toj metamatematici — za razliku od čisto formalnih načina zaključivanja prave matematike — dolazi do primjene sadržajnog zaključivanja, u svrhu dokaza konzistentnosti aksioma."

Kraće rečeno, Hilbert zahtijeva ne samo svodivost sve matematike na formule izvedive iz aksioma, nego uvodi i „matematiku o matematici", metamatematiku. Za više o Hilbertovom programu čitatelja upućujemo na članak [20].

Na nužnost razlikovanja matematike i metamatematike upućuje **Richardov paradoks**. Radi se o paradoksu francuskog matematičara Julesa Richarda (1862.–1956.) kojeg je predstavio 1905. godine. Razmatrao je bilo koji jezik (kao npr. hrvatski) u kojem su definirana aritmetička svojstva prirodnih brojeva. Recimo „prvi prirodni broj" definira svojstvo prvog prirodnog broja, tj. broja 1, a „nije djeljiv bilo kojim prirodnim brojem osim s 1 i samim sobom" definira svojstvo prostog broja. Popis svih takvih mogućih svojstava je očito beskonačan, ali lako je vidjeti da je svaka pojedinačna definicija sastavljena od konačnog broja riječi, a time i konačnog broja znakova. Sada se definicije mogu poredati po duljini na način da će jedna definicija prethoditi drugoj ako je duljina prve manja od duljine druge. U slučaju da dvije definicije imaju jednak broj znakova, presudit će leksikografski uređaj. Richard je zatim preslikao uređeni skup tih svojstava (definicija) na skup prirodnih (tj., u smislu teorije skupova, konačnih kardinalnih) brojeva sa standardnim uređajem, tako što je definiciju s najmanjim brojem znakova i prvom po leksikografskom poretku poistovjetio s brojem 1, sljedeću definiciju u nizu s brojem 2 itd. Budući da tako svakom svojstvu odgovara jedinstven prirodan broj, moguće je da će povremeno prirodan broj dodijeljen svojstvu stvarno i odgovarati tom svojstvu. Na primjer, ako je svojstvo „je djeljiv samo s 1 i sa samim sobom" dodijeljeno broju 28 (ili neki veći, ovisno o tome koliko toj definiciji u leksikografskom poretku prethodi drugih definicija) onda bi to bila istina. Međutim, ako bi tom istom svojstvu bio pridružen broj, primjerice, 17, to bi bila laž. U ovom drugom

slučaju riječ je o Richardovim brojevima. Preciznije, „*n* je Richardov broj" ekvivalentno je s „*n* ne zadovoljava svojstvo naznačeno u definiciji kojoj je pridružen broj *n*". S obzirom na to da je svojstvo da je neki broj Richardov numeričko svojstvo prirodnih brojeva, onda i tom svojstvu odgovara neki prirodan broj *n*. Sada slijedi paradoks: „Je li *n* Richardov broj?" Recimo da je. To je moguće samo ako *n* ne ispunjava svojstvo naznačeno u definiciji kojoj je pridružen broj *n*. Drugim riječima, istinito je samo onda kada *n* nije Richardov broj. Dakle, *n* je Richardov broj ako i samo ako *n* nije Richardov broj [16].

Problem kod Richardovog paradoksa, kao i kod Russellovog, jest „pozivanje na samog sebe" (samoreferiranje). Pokušavajući, među ostalim, riješiti takve probleme razlikovanjem skupova od klasa, Alfred North Whitehead i Bertrand Russell napisali su knjigu *Principia Mathematica* i izdali je u tri dijela, 1910., 1912. i 1913. godine. Cilj tog djela bio je svesti čitavu matematiku na simboličku logiku uz minimalni skup aksioma i pravila zaključivanja. Među ostalim tim djelom su Russell i Whitehead (empirijski) potvrdili *dovoljnost* logičkih pravila zaključivanja kako ih je krajem 19. stoljeća formulirao njemački matematičar i logičar G. Frege [32].

Hilbertov program doživio je velik šok 1931. godine kada je Kurt Gödel (1906.–1978., slika 1.4) pokazao da su Peanovi aksiomi, i svako učinkovito proširenje tih aksioma (uključujući analizu i teoriju skupova), nepotpuni ako su konzistentni. Štoviše, konzistentnost takvog sustava ne može se dokazati unutar njega samoga koristeći samo konačne metode. Gödel je bio američki matematičar i logičar češkog podrijetla. Doktorirao je na Sveučilištu u Beču 1929. godine. Od 1953. bio je profesor na Institutu za napredne studije u Princetonu, SAD. Od ranog djetinjstva bio je jako boležljiv, stoga je tijekom života bio izrazito zabrinut za svoje zdravlje što ga je dovelo do paranoje. To stanje se samo pogoršavalo godinama, te naposlijetku zbog straha od trovanja nije htio pojesti ništa ako njegova žena ne bi prva kušala. Kada se ona razbolila i bila hospitalizirana na duži period, Gödel je prestao jesti i na kraju preminuo od gladi [1].

U svojoj doktorskoj disertaciji 1929. odgovorio je na pitanje koje su postavili David Hilbert i Wilhem Ackerman 1928. godine: Ako skup aksioma definira neki matematički sustav, omogućuju li pravila logičkog zaključivanja da se izvede svaka istinita tvrdnja o tom sustavu i osiguravaju li da se isključivo mogu izvesti istinite tvrdnje? Očekivani odgovor bio je „da", a Gödel je u svojoj disertaciji potvrdio da jest. Gödelov znameniti teorem o potpunosti potvrda je da su načela logike prikladna za dokazivanje istinitih tvrdnji o sustavu na temelju danih aksioma. Preciznije rečeno, Gödelov teorem o potpunosti kaže da za zadani skup aksioma Fregeova logička pravila zaključivanja uvijek generiraju *sve* njihove logičke posljedice (teoreme, propozicije). Međutim, to ne znači da se svaka istinita tvrdnja o prirodnim brojevima može dokazati na temelju aksioma aritmetike, tj. Peanovih aksioma. Godine 1931. Gödel je dokazao svoj znameniti **prvi teorem nepotpunosti**, koji kaže da neoviso o tome kako se formuliraju aksiomi aritmetike, uvijek će postojati tvrdnje o prirodnim brojevima koje se ne mogu dokazati, tj. da će uvijek osim prirodnih brojeva postojati

Slika 1.4: Kurt Friedrich Gödel (*public domain* slika preuzeta s Wikipedije)

i neki drugi objekti koji zadovoljavaju iste aksiome. Drugim riječima, nijedna deduktivna teorija koja obuhvaća aritmetiku prirodnih brojeva nije idealna u smislu da nije dokaziva nijedna neistinita propozicija, ali jesu dokazive sve istinite propozicije. Iste, 1931., godine Gödel je dokazao i **drugi teorem nepotpunosti**, čiji smisao je da se konzistentnost aksiomatskog sustava koji uključuje aritmetiku ne može dokazati unutar samog sustava [32, 9].

Gödelovi dokazi teorema nepotpunosti temelje se na ideji preslikavanja tvrdnji o sustavu aksioma na tvrdnje o prirodnim brojevima. Prvi korak bilo je pridruživanje jedinstvenog broja, kojeg zovemo **Gödelov broj**: simbolu $\neg$ („ne") odgovara Gödelov broj 1, simbolu $\vee$ („ili") broj 2 i t.d. (vidi [35]), svakoj matematičkoj tvrdnji (ili nizu tvrdnji). Ovdje opisujemo malo izmijenjenu verziju izvorne Gödelove sheme, kako su ju predstavili E. Nagel i J. Newman u svojoj knjizi *Gödelov dokaz* (1958.). Započinjemo s 12 elementarnih simbola koji služe kao rječnik za izražavanje osnovnih aksioma i dodijeljeno im je prvih 12 Gödelovih brojeva. Slovima koja predstavljaju varijable (kao npr. $x, y, z, \ldots$) pridružuju se prosti brojevi veći od 12. Dalje se svakoj kombinaciji tih simbola pridružuje vlastiti Gödelov broj. Na primjer, u tvrdnji $0 = 0$ redom imamo simbole s Gödelovim brojevima 6 5 6. Taj niz treba promijeniti u jedinstven broj koji neće biti pridružen nikojem drugom nizu simbola. Da bi to postigao, Gödel uzima prva tri prosta broja (2, 3 i 5), potencira ih na Gödelov broj odgovarajućeg simbola te ih množi. Tako $0 = 0$ postaje $2^6 \cdot 3^5 \cdot 5^6$ odnosno 243 000 000. Na ovaj način nikoje dvije formule neće dobiti isti Gödelov broj zbog jedinstvenosti rastava na proste brojeve, dakle osigurana je injektivnost preslikavanja simboličkih tvrdnji (neovisno o tom jesu li istinite) u prirodne brojeve. Štoviše, Gödel je na analogan način i dokazima (nizovima simboličkih tvrdnji kojima su Gödelovi brojevi pridruženi na upravo opisan način) pridružuje vlastite Gödelove brojeve. Štoviše, i metamatematičke tvrdnje se ovako mogu svesti na prirodne brojeve. Primjerice, (neistinitoj)

formuli $\neq (0 = 0)$ prema gornjem principu pridružen je Gödelov broj $2^1 \cdot 3^8 \cdot 5^6 \cdot 7^5 \cdot 11^6 \cdot 13^9$. Ako bismo sad gledali (istinitu) metamatematičku tvrdnju „prvi simbol formule $\neg(0 = 0)$ je simbol negacije", ona je sad tvrdnja da je u broju $2^1 \cdot 3^8 \cdot 5^6 \cdot 7^5 \cdot 11^6 \cdot 13^9$ prvi eksponent 1, tj. da u broju $2^1 \cdot 3^8 \cdot 5^6 \cdot 7^5 \cdot 11^6 \cdot 13^9$ imamo samo jedan faktor 2. To se pak opet može zapisati simbolički pa i toj tvrdnji odgovara jedinstveni Gödelov broj. Gödel je zatim uočio da se čak i broj neke formule može bez problema supstituirati u nju: Ako uzmemo formulu $\exists x(x = sy)$ (postoji x koji je sljedbenik od y), ona ima Gödelov broj $m \in \mathbb{N}$, možemo m supstituirati na mjesto y i dobiti $\exists x(x = sm)$ (m ima sljedbenika). Označimo Gödelov broj te tvrdnje sa $\sup(m, m, 17)$ (17 je Gödelov broj simbola y). Općenito, $\text{sub}(a, a, c)$ znači da se u formulu s Gödelovim brojem a na sva mjesta na kojima je simbol s Gödelovim brojem c supstituira a. U dokazu prvog teorema nepotpunosti Gödel sad razmatra (metamatematičku) tvrdnju „Formula s Gödelovim brojem $\sup(y, y, 17)$ se ne može dokazati". Toj tvrdnji kao gore opet odgovara neki Gödelov broj n. Sad se ponovi slično: Razmotrimo tvrdnju G: „Formula s Gödelovim brojem $\sup(n, n, 17)$ se ne može dokazati". Tvrdnja G također ima svoj Gödelov broj. No, po definiciji $\sup(n, n, 17)$ je Gödelov broj formule koju dobijemo iz formule Gödelovog broja n i supstituirajući n na sva mjesta na kojima je u toj formuli simbol s Gödelovom brojem 17. Ta formula je upravo G pa jedinstvenost faktorizacije na proste faktore povlači da G govori o samoj sebi, tj. kaže sama o sebi da se ne može dokazati. Ako bi se G mogla dokazati, postojao bi niz formula koji dokazuje formulu s Gödelovim brojem $\sup(n, n, 17)$, no to je točno negacija od G. Budući da u konzistentnom aksiomatskom sustavu G i $\neg G$ ne mogu istovremeno biti istinite, slijedi da je G neodlučiva. Budući da je G očito lažna, vidimo da postoje neodlučive, a istinite tvrdnje u sustavu prirodnih brojeva. Gödel je dalje pokazao da koje god aksiome dodali da postignemo dokazivost G, opet će se (na sličan način) moći konstruirati istinita nedokaziva tvrdnja. Tako možemo nastaviti u beskonačnost, dodavati aksiome, ali uvijek će ostati nedokazive istinite tvrdnje. Dakle, svaki aksiomatski sustav koji sadrži Peanovu aritmetiku je nepotpun[35].

Vratimo se natrag na Hilberta. U svojim spisima o logici, Hilbert je naglasio ključnu važnost onoga što je nazvao *Entscheidungsproblem* (problem odlučivanja). To je bio problem problem pronalaska računalnog programa koji će kao ulaz uzeti opis formalnog jezika i matematičku tvrdnju u tom jeziku i vratiti kao izlaz "istina" ili "laž", ovisno o tome je li tvrdnja istinita ili lažna. Program ne treba opravdati svoj odgovor, niti pružiti dokaz, važno je jedino da uvijek da točan odgovor. Takav bi računalni program bio u mogućnosti odlučiti je li npr. hipoteza kontinuuma istinita. Alan Turing (1912.–1954., slika 1.5) je dokazao[15] da takav program ne može postojati nekoliko godina nakon objave Gödelovog rada. Višenamjenska digitalna računala u Turingovom radu bile su matematičke apstrakcije, ali ga je zaintrigirala mogućnost građenja pravih. Ta razmišljanja morala su

[15]Ekivalentan rezultat, također 1936. godine, dobio je nezavisno od Turinga i američki matematičar i logičar Alonzo Church (1903.–1995.).

se zaustaviti zbog Drugog svjetskog rata tijekom kojeg je Turing odigrao ključnu ulogu u dešifriranju njemačkih, tajnih, vojnih kodova. U slobodno vrijeme razmišljao je o tome kako bi računala mogla biti napravljena tako da igraju dobar šah i ponašaju se inteligentno. Kada je rat završio napisao je izvješće u kojem je pokazao kako izgraditi računalo pomoću dostupne tehnologije. Zaposlio se na Sveučilištu u Manchesteru radeći na računalu koje se tamo gradilo, ali policija u Manchesteru ga je uhitila kada je saznala za njegovu homoseksualnu orijentaciju. Bio je osuđen za „tešku nepristojnost“ i prisiljen na „tretman“ sa ženskim spolnim hormonima. Umro je od trovanja cijanidom dvije godine kasnije. Pretpostavlja se da je riječ o samoubojstvu [25].

Slika 1.5: Alan Turing (*public domain* slika preuzeta s Wikipedije)

Turing je 1935. uveo koncept stroja, koji se danas naziva **Turingov stroj**, i dokazao postojanje univerzalnog stroja: stroja koji je, s obzirom na odgovarajući kod, sposoban simulirati rad bilo kojeg drugog Turingovog stroja. Turingova definicija izračunljivosti ne ovisi o pojmu dokaza i dovodi do mnogih zanimljivih pojmova, teorema i još neriješenih problema.

Definicija 1. *Turingov stroj je uređena sedmorka* $(Q, S, T, b, q_0, F, \delta)$*, pri čemu je:*

- $Q = \{q_0, q_1, \ldots, q_N\}$ *konačan skup stanja,*

- *S konačan skup znakova s kojima stroj radi (abeceda trake),*
- *T konačan skup znakova koji se mogu naći na traci prije početka rada stroja (ulazna abeceda); $T \subset S$,*
- *$b \in S \setminus T$ tzv. „prazan" simbol; oznaka da je polje prazno,*
- *$q_0 \in Q$ početno stanje rada stroja,*
- *$F \subseteq Q$ skup završnih stanja i*
- *$\delta : Q \times S \to Q \times S \times \{S, L, D\}$, gdje S označava „stani", L „lijevo", a D „desno".*

Stroj ima beskonačnu traku (koja predstavlja hard disk) i glavu koja se kreće po toj traci za jedno mjesto ulijevo ili udesno, te čita podatke s trake i zapisuje nove. Stanja predstavljaju radnu memoriju i ima ih proizvoljno, ali konačno mnogo. Njih određujemo prilikom sastavljanja stroja, dok se po traci možemo kretati koliko god želimo bez da smo unaprijed predvidjeli koliko je duga. Na početku rada stroja na traci se nalazi zapis opisan ulaznom abecedom koji je analogon ulaznim podacima programa. Turingov stroj nalazi se u stanju q na nekoj poziciji na traci odakle je pročitao znak s. U ovisnosti o ta dva parametra on prelazi u novo stanje q', zapisuje novi znak s' na traku na poziciju na kojoj se nalazi, te pomiče glavu za jedno mjesto ulijevo ili udesno ili ostane stajati na istom mjestu, tj. obavi pomak iz skupa $\{S, L, D\}$. Jedan korak Turingovog stroja možemo opisati petorkom (q, s, q', s', m), pri čemu $q, q' \in Q, s, s' \in S, m \in \{S, L, D\}$. Proces rada Turingovog stroja δ u potpunosti je određen konačnim skupom petorki opisanog oblika. Definiramo da stroj staje s radom kada dođe u završno stanje i napravi pomak „S", tj. kad funkcija δ izvrši preslikavanje $(q_i, x) \to (q_p, y, S)$, pri čemu $x, y \in S, q_i \in Q, q_p \in F$ [31].

Koncept Turingovog stroja ima filozofsko značenje zbog sljedećih analogija:

$$\frac{\text{Turingov stroj}}{\text{njegova traka}} = \frac{\text{organizam}}{\text{njegov okolis}},$$

$$\frac{\text{univerzalan Turingov stroj}}{\text{ulazni kod}} = \frac{\text{ljudsko bice}}{\text{njegovo znanje}}.$$

Ove analogije su potkrijepljene činjenicom da za svaki računalni postupak (algoritam) u stvarnom svijetu postoji Turingov stroj koji može izvesti taj postupak. Univerzalni Turingov stroj δ je teorijski model programibilnog računala [24].

Vezan za Turingov stroj je jedan poznati neodlučivi problem, tzv. *halting problem* (**problem zaustavljanja**). Dobro je poznato da prilikom pisanja računalnog programa treba misliti na to da se može dogoditi da se u nekim slučajevima program ne izvrši nego uđe u beskonačnu petlju. Na pitanje postoji li algoritam koji za svaki računalni program i svaki ulaz (*input*) tog programa može odlučiti hoće li se program zaustaviti ili ne, odgovor

„ne' je dao Turing 1936. godine. Ideja Turingovog dokaza kreće od osnovnih elemenata: ulaz, program (skup pravila koji djeluju na ulaz i vraćaju izlaz) i izlaz. Turing je pretpostavio da je moguće napisati program HALT koji, za svaki zadani program i pripadni ulaz, može odrediti hoće li se izvođenje tog programa zaustaviti ili ne:

$$\text{HALT(program, ulaz)} = \begin{cases} \text{izlaz DA}, & \text{ako se program zaustavi} \\ \text{izlaz NE}, & \text{inače} \end{cases}.$$

Ako takav program HALT postoji, može se napisati novi program OPPOSITE koji analizira programe koji za ulaz imaju sami sebe, , tj. koji se zaustavlja ako i samo ako se zadani program ne zaustavlja:

$$\text{OPPOSITE(program)} = \begin{cases} \text{zaustavlja se}, & \text{ako HALT(program, program) vrati NE} \\ \text{beskonačna petlja}, & \text{inače} \end{cases}.$$

Međutim, što se dogodi ako program OPPOSITE pokušamo pokrenuti na samom sebi? Ako se zaustavi, onda mora upasti u beskonačnu petlju, a ako upadne u beskonačnu petlju, onda se mora zaustaviti (uočimo opet analogiju s Russellovim paradoksom). Zbog ove kontradikcije slijedi da program HALT ne može postojati, dakle problem zaustavljanja je neodlučiv [34].

Problem zaustavljanja posebno je važan, ne samo jer je konkretniji od primjera s Gödelovim numeriranjem, nego se i za mnoge danas poznate neodlučive probleme dokaz neodlučivosti svodi na njega. Tako se i Gödelov 1. teorem nepotpunosti može dokazati iz Turingova rezultata. A što je s hipotezom kontinuuma, od koje smo krenuli? Ona se našla na Hilbertovom popisu 23 problema kao prvi problem. Prvi korak ka rješenju napravio je Kurt Gödel 1940. godine dokazavši da hipoteza ne može biti opovrgnuta u standardnom Zermelo-Fraenkelovom aksiomatrskom sustavu, čak ni ako se usvoji aksiom izbora.[16] 1963. godine Paul Cohen (1934.–2007.) je pokazao da ju se uz iste ove aksiome ne može dokazati. Stoga, hipoteza kontinuuma se ne može ni dokazati ni opovrgnuti u Zermelo-Fraenkelovom aksiomatrskom sustavu, odnosno problem hipoteze kontnuuma je neodlučiv [21].

U drugom poglavlju predstavit ćemo nekoliko poznatih, zanimljivih, a dokazano neodlučivih problema, tj. problema za koje poput problema zaustavljanja ne postoji algoritam koji bi u svakom slučaju koji je uključen danim problemom dao odgovor 'da' ili 'ne' ovisno o tome je li za taj slučaj problem rješiv..

[16] Aksiom izbora je aksiom koji se uobičajeno dodaje Zermelo-Fraenkelovom sustavu aksioma: Za svaku familiju nepraznih i međusobno disjunktnih skupova postoji skup koji sa svakim skupom iz te familije ima točno po jedan zajednički element.

Poglavlje 2

Primjeri neodlučivih problema

2.1 Igra života

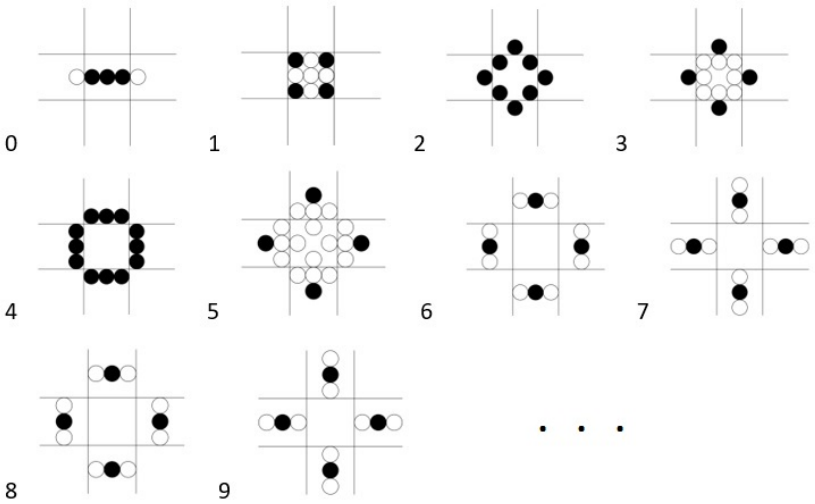
Igru života osmislio je 1970. godine engleski matematičar John Horton Conway (1937.–2020.). Za igru nije potreban nijedan igrač. Igra se na beskonačnoj ploči ćelija kvadratnog oblika, a u svakom trenutku svaka ćelija je ili živa ili mrtva. U početnom trenutku $t = 0$ mi odlučujemo koje će ćelije biti žive, ali u svakom sljedećem trenutku $t \neq 0$ nemamo više što raditi jer se ćelije ponašaju po sljedećim pravilima:

- Rođenje: Ćelija koja je mrtva u trenutku t postaje živa u trenutku $t + 1$ ako su joj točno tri susjedne ćelije bile žive u trenutku t.
- Smrt zbog prenapučenosti: Ćelija koja je živa u trenutku t i barem četiri od njenih osam susjeda su također živi u trenutku t, bit će mrtva u trenutku $t + 1$.
- Smrt zbog izloženosti: Ćelija koja je živa u trenutku t, ali u tom trenutku ima samo jednog živog susjeda ili nema nijednog, također će biti mrtva u trenutku $t + 1$.
- Opstanak: Ćelija koja je živa u trenutku t bit će živa i u trenutku $t + 1$ ako i samo ako ima dva ili tri živa susjeda u trenutku t.

Iako su pravila vrlo jednostavna, igra može generirati mnogo različitih uzoraka. Neki uzorci su stabilni i nikada se ne mijenjaju, neki osciliraju naprijed-nazad u beskonačnoj petlji, neki zauvijek putuju u mreži, mnogi jednostavno nestaju, ali neki od uzoraka zauvijek rastu. Pogledajmo neke.

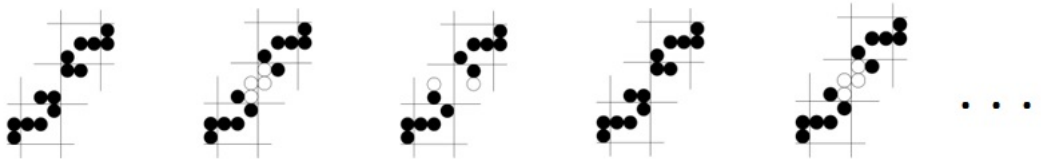
Tipičan uzorak koji se može pojaviti je uzorak semafora. Ukoliko igru započnemo jednostavnom linijom od pet ćelija, igra će generirati uzorak prikazan na slici 2.1. Krugovi ispunjeni crnom bojom predstavljaju ćelije koje će u sljedećoj generaciji preživjeti, a oni ispunjeni bijelom bojom one koji će umrijeti. U generaciji 0, vanjske ćelije imaju samo

jednog živog susjeda i zbog toga umiru, a unutarnje ćelije imaju po dva živa susjeda pa preživljavaju do generacije 1. Također, rodile su se i nove ćelije jer su imale tri živa susjeda. U generaciji 1, preživljavaju isključivo ćelije na krajevima jer imaju točno tri živa susjeda, ostale ćelije umiru zbog prenapučenosti. Rađaju se četiri nove ćelije. Analogno se nastavlja dalje. Od generacije 6 na dalje primjećujemo uzorak semafora. Četiri zasebne linije od tri ćelije nikada se više neće dotaknuti – došli smo do beskonačne petlje.



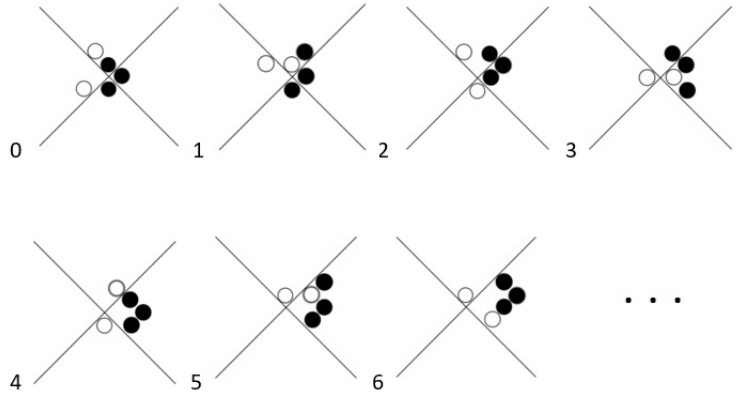
Slika 2.1: Uzorak semafora

To je bio jednostavan primjer konfiguracije koja ponavlja svoj život s periodom 2. Na slici 2.2 prikazan je primjer uzorka koji se ponavlja s periodom 3.



Slika 2.2: Uzorak kruga života s periodom 3

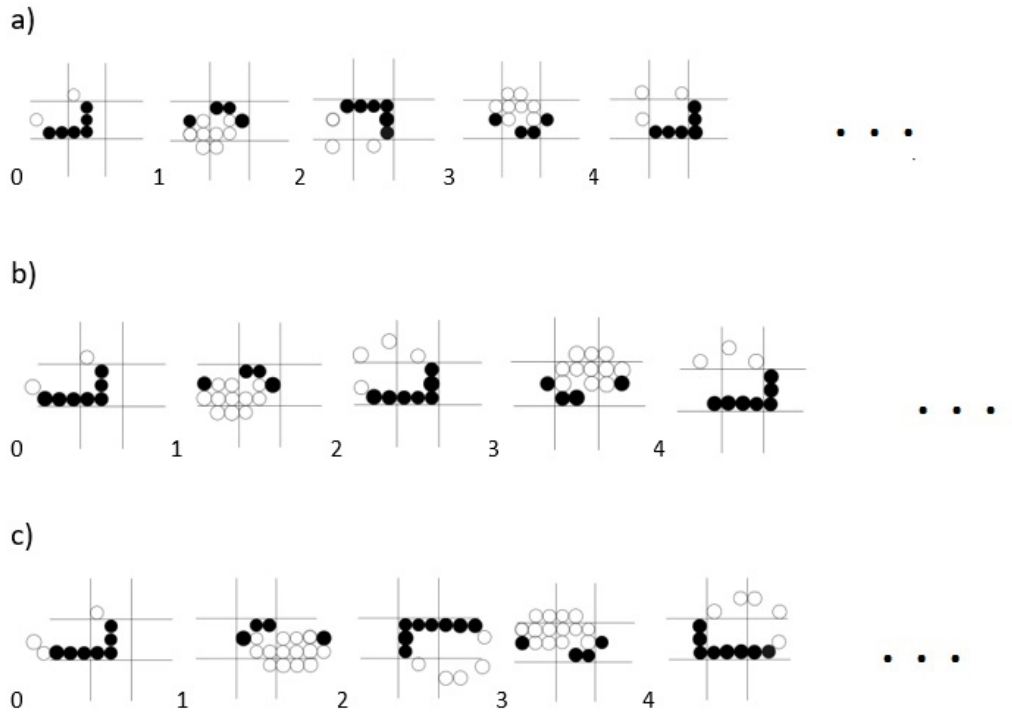
Također, često se pojavljuje i konfiguracija klizača. Takvo je ime dobila jer početni lik izgleda kao da „klizi“ kroz prostor. Na slici 2.3 možemo vidjeti primjer klizača.



Slika 2.3: Klizač

Postoje razne vrste klizača, ali jedan od najpoznatijih je svemirski brod, koji klizi horizontalno. Lagani svemirski brod se generalizira u srednje teški i teški svemirski brod (slika 2.4) a druge, duže verzije su se pokazale nestabilnima. Kasnije se pokazalo kako proizvoljno dugi svemirski brodovi ipak mogu putovati ako ih prate manji brodovi. Svi svemirski brodovi se kreću u smjeru istoka. tj. udesno.

Postoji li neki način da odredimo sudbinu početnog uzorka? Hoće li s vremenom nestati, postati statičan ili možda zauvijek rasti? Na ova pitanja nemoguće je naći općenit odgovor. Conway je postavio hipotezu da ne postoje neograničeno rastuće ograničene početne konfiguracije i ponudio nagradu od 50 $ onomu tko dokaže ili opovrgne tu tvrdnju. 1970. godine jedna grupa s MIT-a, koju je predvodio R. W. Gosper, osvojila je nagradu jer je pronašla uzorak klizača – pištolj koji emitira novi uzorak klizača svakih trideset generacija, i tako u beskonačnost. S obzirom na to da taj uzorak raste u beskonačnost, slijedi da postoje ograničeni početni uzorci u Igri života koji će rasti zauvijek.



Slika 2.4: (a) Lagani, (b) srednje teški, (c) teški svemirski brod

Otkriće pištolja potaknulo je otkriće mnogih drugih uzoraka od kojih je možda i najzanimljiviji primjer pištolj koji ispucava svemirske brodove koji reprezentiraju proste brojeve. Taj uzorak naziva *primer* je konstruirao Dean Hickerson 1991. godine. Ne čini se intuitivno da se prosti brojevi, koji su naizgled slučajni i nepredvidivi, mogu generirati ovim, relativno jednostavnim, uzorkom u potpuno determinističkoj Igri života. Pištolj ulijevo ispaljuje lagane svemirske brodove koji predstavljaju proste brojeve. Ostale brojeve uništavaju klizači koji oponašaju Erastotenovo sito, odnosno lagane svemirske brodove unište klizači koji predstavljaju pozitivne cijele brojeve onda kada lagani svemirski brod predstavlja višekratnik toga broja. Prirodan broj N je prost ako i samo ako lagani svemirski brod uspije proći kraj lijevog donjeg ruba pištolja pri generaciji $120N$. Kasnije je *primer* dorađen za generaciju raznih podvrsta prostih brojeva (Mersenneove, Fermatove, ...) i raznih n-torki prostih brojeva (parovi blizanci, parovi oblika $(p, p + 2k)$, ...). Konkretno, nedugo nakon što je osmislio *primer*, Hickerson je shvatio da može pričvrstiti pištolj na

njegov donji lijevi kut kako bi ga pretvorio u kalkulator brojeva blizanaca[1] dopuštajući svakom laganom svemirskom brodu da prođe kraj lijevog donjeg kuta pištolja ako i samo ako je drugi lagani svemirski brod prošao tamo 240 generacija ranije. Slično, Jason Summers je 2000. godine konstruirao kalkulator Fermatovih brojeva[2] tako što pištolj ispaljuje klizač na lagani svemirski brod svake generacije u obliku $120(2N + 1)$.

Osim problema vezanih za proste brojeve i mnogi drugi matematički problemi mogu se svesti na pitanja u kontekstu Igre života. Njihova rješivost, odnosno odlučivost o postojanju njihova rješenja, tako se svodi na osnovno pitanje o Igri života: Može li se za dani početni uzorak i dani drugi uzorak utvrditi (nekim algoritmom) hoće li početni uzorak ikad rezultirati tim drugim uzorkom? No, dokazano je da je Igra života je neodlučiva. To je jednostavna posljedica činjenice da Igra života može simulirati univerzalni Turingov stroj i neodlučivosti problema zaustavljanja [25, 3, 18, 27].

[1] Par prostih brojeva naziva se blizancima ako im je razlika 2.

[2] Fermatovi brojevi su prosti brojevi oblika $2^{2^n} + 1$, pri čemu je $n \in \mathbb{N}$.

2.2 Wangove pločice

Jedan od temeljnih problema u teoriji popločavanja[3] je odlučiti može li se, s obzirom na dani skup pločica i pravilo popločavanja popločati ravnina. Jedna varijanta tog problema zove se problem domina i 1961. godine ju je postavio Hao Wang. Wang je promatrao kvadratne pločice obojane različitim bojama i pokušavao ih složiti bez da ih je rotirao, tako da se boje na rubovima koji se dodiruju, slažu. Robert Berger je 1966. godine prvi dokazao da je taj problem neodlučiv, a kasnije su se brojni matematičari bavili time pa postoji mnogo dokaza od kojih je najpoznatiji onaj Raphaela Robinsona.

Definicija 2. *Neka je C konačan skup kojeg zovemo skupom boja. Wangova pločica je kvadratna pločica podijeljena dijagonalama na četiri dijela N, S, E, W koji su obojani bojama iz C.*

Primjer Wangovih pločica vidimo na slici 2.5. Skup C općenito može biti skup boja, uzoraka, simbola ili brojeva.

Slika 2.5: Wangove pločice

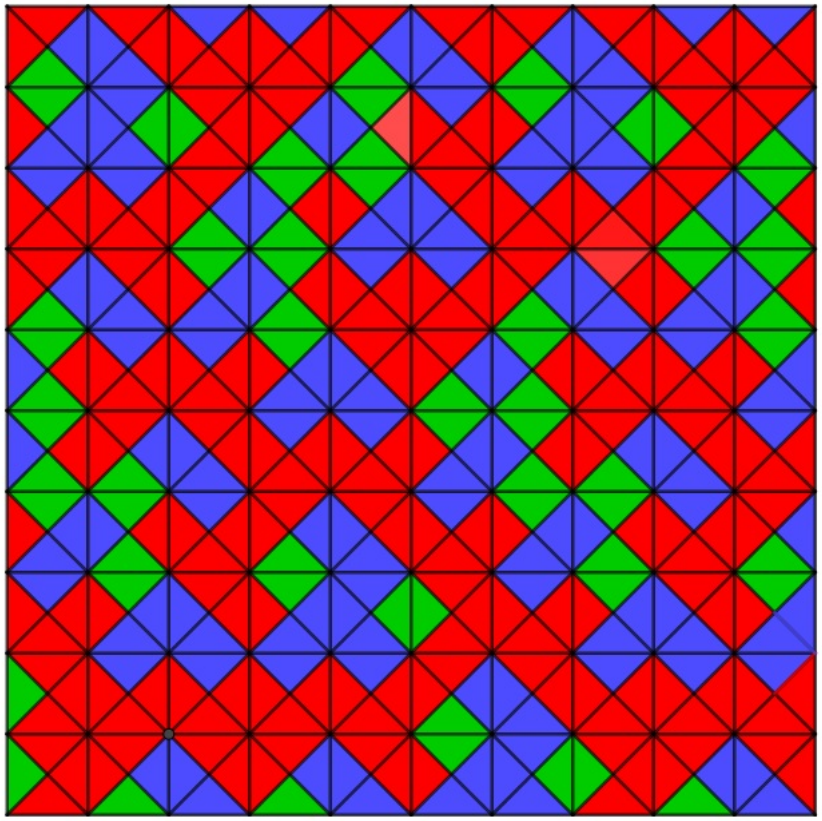
Definicija 3. *Neka je $P = Z^2$,[4], a τ neki konačan skup Wangovih pločica. Konfiguracija x ravnine pridružuje svakom elementu iz P pločicu iz τ.*

Dakle, konfiguracija je preslikavanje $x : P \to \tau$. Umjesto čitave ravnine moguće je razmatrati i popločavanje njenog dijela (kao npr. ña slici 2.6), što se reprezentira funkcijom istog tipa za prikladni $P \subseteq \mathbb{Z}^2$; u tom slučaju umjesto o konfiguraciji govorimo o uzorku. Popločavanje ravnine prema τ je konfiguracija koja svakom elementu ravnine pridružuje pločicu iz τ takvu da se boja svake njene susjedne pločice podudara s bojom pločice iz τ na njihovom zajedničkom rubu. Preciznije, popločavanje ravnine skupom Wangovih pločica τ je konfiguracija $x : P \to \tau$ takva da vrijedi:

[3]Popločavanje ravnine je pokrivanje ravnine kopijama jednog ili više likova, pločica, bez preklapanja i praznina.

[4]Dakle, ravnina je opskrbljena rešetkom točaka s cjelobrojnim koordinatama u Kartezijevom koordinatnom sustavu. Podrazumijeva se da je jedinična duljina jednaka duljini brida Wangove pločice.

- ako $(i, j) \in P$ i $(i + 1, j) \in P$ onda $x(i, j)(E) = x(i + 1, j)(W)$,
- ako $(i, j) \in P$ i $(i, j + 1) \in P$ onda $x(i, j)(N) = x(i, j + 1)(S)$.



Slika 2.6: Primjer popločavanja konačnog kvadrata prema jednom skupu Wangovih pločica

Uočimo da iz definicije slijedi da Wangove pločice pri popločavanju ne smijemo rotirati (što je inače općenito dozvoljeno kod razmatranja popločavanja ravnine). Problem domina se stoga svodi na pitanje može li se ravnina popločati prema gore opisanoj konfiguraciji x danim skupom Wangovih pločica τ. Vrijedi sljedeća propozicija [17]:

Propozicija 2. *τ popločava ravninu ako i samo ako za svaki prirodan broj n, skup Wangovih pločica τ popločava kvadrat veličine $n \times n$.*

Ova propozicija omogućava nam da u nekim slučajevima lako dokažemo kada τ ne popločava ravninu: Za svaki n tražimo način popločavanja kvadrata $n \times n$ prema τ, ako

za neki n nije moguće popočati kvadrat, onda je nemoguće popločati ravninu prema τ. Također, lako je pokazati i kad se neka ravnina može popločati periodično[5]: ako se za neki n pronađe popločavanje kvadrata veličine $n \times n$, onda je moguće periodično popločati ravninu prema τ (jednostavno taj kvadrat koristimo kao pločicu standardnog kvadratnog popločavanja). No, odlučiti postoji li neperiodično popločavanje ravnine prema τ općenito nije moguće. Prvi neperiodičan skup Wangovih pločica[6] pronašao je Berger 1966. godine, a sastojao se od 20426 pločica. Najmanji do danas pronađen neperiodičan skup Wangovih pločica sastoji se od 11 pločica obojanih u 4 boje, a otkrili su ga matematičari Jeandel i Rao 2015. godine. Također su dokazali da ne postoji takav skup s manje od 11 pločica ili manje od 4 boje.

Kao što je već navedeno, Berger je prvi dokazao da je problem Wangovih pločica neodlučiv, odnosno da vrijedi sljedeći teorem:

Teorem 1. *Ne postoji algoritam koji odlučuje može li dani skup Wangovih pločica popločati ravninu.*

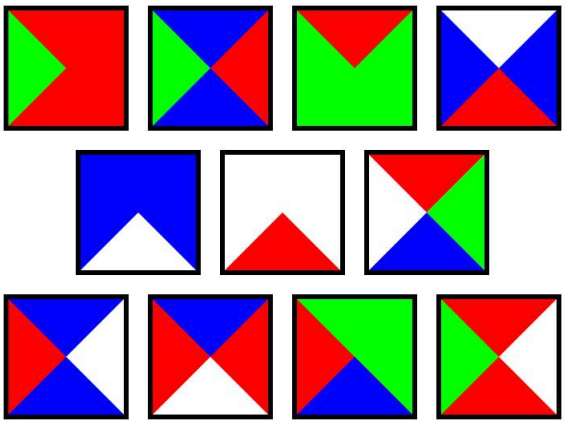
Bergerov teorem zapravo kaže: Neka je τ skup Wangovih pločica. Onda su moguća tri različita slučaja:

- τ ne popločava ravninu;
- τ popločava ravninu i postoji periodičan uzorak[7], kao npr. popločavanje kopijama kvadrata sa slike 2.6;
- τ popločava ravninu isključivo aperiodično, kao npr. skup τ na slici 2.7; za više o takvim popločavanjima upućujemo na web-stranicu [30].

[5]Popločavanje ravnine je periodično ako posjeduje translacijsku simetriju u dva nekolinearna smjera.

[6]Skup pločica koji omogućuje samo neperiodična popločavanja ravnine naziva se neperiodičnim.

[7]Popločavanje ravnine je periodično ako posjeduje translacijsku simetriju u dva neparalelna smjera. Za konfiguraciju x ta se definicija svodi na to dapostoji $p \in \mathbb{N}$ takav da $x(i, j) = x(i \mod p, j \mod p)$ za sve $i, j \in \mathbb{N}$.



Slika 2.7: Skup od 11 Wangovih pločica (slika preuzeta s `https://commons.wikimedia.org/wiki/File:Wang_11_tiles.svg`, Free Art License)

Robinsonov, a u biti i Bergeov, dokaz neodlučivosti problema domina svode se na — kao što je i kod Igre života — na nerješivost problema zaustavljanja za Turingov stroj. [25, 17]

2.3 Hilbertov deseti problem

Hilbertov deseti problem je problem pronalaska računalnog algoritma koji će za danu diofantsku jednadžbu[8] s cjelobrojnim koeficijentima odlučiti ima li cjelobrojna rješenja. To je deseti problem na listi problema koje je Hilbert predstavio 1900. godine. Hilberta nije zanimao pronalazak samih rješenja, nego samo zaključak o njihovoj egzistenciji putem jednog jedinog algoritma za sve jednadžbe. Primjerice, za diofantsku jednadžbu $x^3 + y^3 = z^3$ dokaz velikog Fermatovog teorema povlači da ona nema rješenja, dok diofantska jednadžba $x^2 + y^2 = z^2$ ima rješenja (pitagorejske trojke). Ono što Hilbert pita u svom desetom problemu je postoji li način (algoritam) koji bi za svaki polinom $P(x_1, \ldots, x_n)$ s cjelobrojnim koeficijentima (i prozivoljnim brojem n varijabli) utvrdio postoji li rješenje diofantske jednadžbe $P(x_1, \ldots, x_n) = 0$. Matiyaševič je 1970. godine dovršio dokaz da takav algoritam ne postoji, tj. da je Hilbertov deseti problem neodlučiv. Mi ćemo ovdje dati glavne ideje moderniziranog dokaza iste tvrdnje prema [7].

Prvo primijetimo da ako ne postoji algoritam za utvrđivanje ima li proizvoljna diofantska jednadžba *pozitivna* rješenja, tj. rješenja u skupu prirodnih brojeva, onda automatski slijedi da ne postoji algoritam koji utvrđuje ima li ta jednadžba rješenja. Naime, zbog Lagrangeovog teorema o četiri kvadrata[9] slijedi da diofantska jednadžba $P(x_1, \ldots, x_n) = 0$ ima rješenja u skupu prirodnih brojeva ako i samo ako diofantska jednadžba $P(1 + i_1^2 + j_1^2 + k_1^2 + l_1^2, \ldots, 1 + i_n^2 + j_n^2 + k_n^2 + l_n^2) = 0$ ima rješenja u skupu cijelih brojeva. Sad definirajmo što su diofantski skupovi i funkcije:

Definicija 4. *Skup S uređenih n-torki prirodnih brojeva se naziva diofantskim ako postoji polinom s cjelobrojnim koeficijentima $P(x_1, \ldots, x_n, y_1, \ldots, y_m)$ s $m \geq 0$, takav da je $\langle x_1, \ldots, x_n \rangle \in S$ ako i samo ako postoje prirodni brojevi $y_1, \ldots, y_m$ za koje vrijedi da je $P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0$. Realna funkcija f s n prirodnih varijabli naziva se diofantskom ako je njezin graf diofantski skup.*

Primjerice, skup parnih prirodnih brojeva je diofantski jer je broj n paran ako i samo ako za neki prirodan broj m vrijedi $n = 2m$, dakle, ako i samo ako (n, m) zadovoljava diofantsku jednadžbu $n - 2m = 0$.

Zatim se dokazuje da je skup $\{(k, l, m) \in \mathbb{N}^3 : k = l^m\}$ diofantski, tj. da je funkcija zadana s $f(l, m) = l^m$ diofantska. Zatim se dokazuje i da je funkcija diofantska ako i samo ako je rekurzivna:

Definicija 5. *Definiramo primitivne funkcije c, s i u_i^n formulama*

$$c(x) = 1,$$

[8] Diofantska jednadžba je polinomijalna jednadžba u jednoj ili više nepoznanica čija se rješenja traže u prstenu cijelih brojeva.

[9] Svaki prirodan broj je zbroj četiri kvadratna broja.

$$s(x) = x + 1,$$

$$u_i^n(x_1, \ldots, x_n) = x_i.$$

Funkcija je rekurzivna ako se može iz primitivnih funkcija dobiti iterativnom primjenom triju operacija:

- ***Kompozicija*** *funkcija* $g_1, \ldots, g_m$ *i* $f(t_1, \ldots, t_m)$ *je funkcija* h*:*
$$h(x_1, \ldots, x_n) = f((g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)).$$

- ***Primitivna rekurzija*** *funkcija* f *i* g *daje funkciju* $h(x_1, \ldots, x_n, z)$ *koja zadovoljava sljedeće jednadžbe:*
$$h(x_1, \ldots, x_n, 1) = f(x_1, \ldots, x_n),$$
$$h(x_1, \ldots, x_n, t + 1) = g(t, h(x_1, \ldots, x_n, t), x_1, \ldots, x_n).$$
Kada je $n = 0$*, onda* f *postaje konstanta pa* h *dobivamo direktno iz* g*.*

- ***Minimizacija*** *funkcija* f *i* g *daje funkciju:*
$$h(x_1, \ldots, x_n) = \min_y[f(x_1, \ldots, x_n, y) = g(x_1, \ldots, x_n, y)],$$
uz pretpostavku da za svaki $x_1, \ldots, x_n$ *postoji barem jedan* y *koji zadovoljava jednadžbu* $f(x_1, \ldots, x_n, y) = g(x_1, \ldots, x_n, y)$*.*

Naposlijetku, enumeriraju se svi diofantski skupovi, tako da dobivamo niz diofantskih skupova $(D_n)_{n\in\mathbb{N}}$. Može se pokazati

Teorem 2 (Teorem univerzalnosti)**.** *Skup* $\{(n, x) : x \in D_n\}$ *je diofantski skup.*

No, budući da su svi diofantski skupovi u nizu $(D_n)_{n\in\mathbb{N}}$, također slijedi da skup $V = \{n \in \mathbb{N} : n \notin D_n\}$ nije diofantski (uočimo opet sličnost s Russellovim paradoksom). Detalje dosad opisanog dijela dokaza možete naći u članku [7], a mi ćemo sada završiti dokaz neodlučivosti Hilbertovog problema.

Teorem 3. *Funkcija* $g(n, x)$ *definirana s:*
$$g(n, x) = 1 \text{ ako } x \notin D_n,$$
$$g(n, x) = 2 \text{ ako } x \in D_n,$$
nije rekurzivna.

Dokaz. Kako je već rečeno, ako je g rekurzivna, onda je i diofantska. To znači da vrijedi

$$y = g(n, x) \Leftrightarrow (\exists y_1, \ldots, y_m)P(n, x, y, y_1, \ldots, y_m) = 0.$$

. Međutim, iz toga slijedi:
$$V = \{x|(\exists y_1, \ldots, y_m)P(x, x, 1, y_1, \ldots, y_m) = 0\}$$
što je u kontradikciji s time da V nije diofantski. □

Teorem 4. *Hilbertov deseti problem nije rješiv.*

Dokaz. Prema teoremu univerzalnosti možemo pisati:

$$x \in D_n \Leftrightarrow (\exists z_1, \ldots, z_k) P(n, x, z_1, \ldots, z_k) = 0,$$

pri čemu je P neki polinom. Pretpostavimo da postoji algoritam koji može provjeriti ima li diofantska jednadžba cjelobrojna rješenja. Tada bi za dane n, x taj algoritam mogao provjeriti je li $x \in D_n$, tj. ima li rješenje jednadžba

$$P(n, x, z_1, \ldots, z_k) = 0.$$

Tada bi se algoritam mogao upotrijebiti i za izračunavanje $g(x, n)$. Budući da su rekurzivne funkcije upravo one koje su izračunljive, slijedi da je g rekurzivna, što je kontradikcija s prethodnim teoremom, dakle pretpostavka da je Hilbertov deseti problem rješiv je netočna. □

Spomenimo ovdje da se izvorni Matiyaševičev dokaz svodi na nerješivost problema zaustavljanja: Uz diofantske skupove definiraju se i „izračunljivo prebrojivi" (*computably enumerable*) skupovi koji odgovaraju Turingovom stroju, a zatim se pokazuje da su ti skupovi jednaki [28, 36].

2.4 *Magic: The Gathering*

Magic: The Gathering je stolna i digitalna kartaška igra koju je osmislio Richard Garfield 1993. godine. Igrač u igri *Magic* preuzima ulogu *Planeswalkera*, moćnog čarobnjaka koji može putovati između dimenzija *Multiverzuma*, vodeći bitku s drugim igračima pomoću čarolija, raznih artefakata i prizivanjem stvorenja, ovisno o karti koju izvuče. Igrač najčešće pobjeđuje svoga protivnika bacanjem čarolija i napadima sa stvorenjima kako bi nanio štetu protivnikovom – ukupnom životnom broju – s ciljem da ga smanji s 20 na 0. *Magic* mogu igrati dva ili više igrača, bilo uživo s kartama bilo digitalno preko računala, pametnog telefona ili tableta.

Alex Churchill je softverski inženjer na Sveučilištu Cambridge, ali i strastveni dizajner igara. Odrastao je igrajući, između ostalog, kanastu, bridž, mahjong i scrabble, a na svojim kućnim policama ima više od 250 društvenih igara. U članku [6], Churchill, Stella Biderman i Austin Herrick su dokazali

Teorem 5. *Problem određivanja pobjednika u igri Magic: The Gathering ako su svi preostali potezi prisilni je neodlučiv.*

Ključan korak dokaza tog teorema je konstrukcija univerzalnog[10] Turingovog stroja unutar same igre (za slučaj dva igrača). Za to su potrebna tri osnovna elementa: traka koja kodira izračun, kontroler za određivanje sljedeće radnje na temelju trenutnog stanja i glava za čitanje/pisanje. Churchill je najprije kodirao različite moći i svojstva karata u niz koraka. Koristio je žetone, koji su predstavljali stvorenja, za kodiranje vrpce te ih označio zelenom i bijelom bojom pažljivo kontrolirajući svojstva snage i jakosti koja su opisana na kartama. Zatim je pokrenuo igru koju su igrala dva igrača (Alice i Bob). Kako bi pronašao scenarij u kojem je nemoguće predvidjeti pobjednika, stvorio je rijetku situaciju u kojoj su igrači primorani odigrati određene karte (preostali su im samo prisilni potezi). Uobičajno je u normalnoj igri *Magic* prisilno izvlačiti niz karata tri ili četiri puta za redom, a sada je to Churchill proširio na milijune prisilnih izbora u nizu. Inače bi igrači imali mnogo više taktičkih i strateških izbora tijekom igre, a i faktor sreće bi imao veću ulogu, ali jednom kada je Turingov stroj postavljen, tu igru ne igraju više ljudi. Zatim je pokazano da jedan od igrača, recimo Alice, pobjeđuje u toj igri ako i samo ako se odgovarajući Turingov stroj zaustavi. Neodlučivost problema zaustavljanja onda povlači da vrijedi gore navedeni teorem. Time je pokazano da je prepoznavanje tko će pobijediti čak i u igri u kojoj nijedan igrač nema netrivijalnih mogućnosti odabira neodlučivo, pa je pitanje optimalne strategije bar toliko teško (u smislu računske složenosti) koliko i neodlučivi problem zaustavljanja. Štoviše, kako se navodi u zaključnom dijelu članka, time je pokazano da je igra *Magic: The Gathering* računski najsloženija do sad proučavana igra. [23, 26].

[10] Turingov stroj je univerzalan ako može simulirati rad svakog Turingovog stroja sa svakim ulazom.

Poglavlje 3

Zaključak

Postoji „rupa” u temeljima matematike zbog koje nikada nećemo znati sve sa sigurnošću – uvijek će postojati tvrdnje koje nije moguće ni dokazati ni opovrgnuti. Iako je, među ostalim, put do ovog otkrića doveo i do jedne od najvećih kriza u povijesti matematike, doveo je i do mnogih vrijednih rezultata. Ključan događaj bio je znameniti Hilbertov govor 1900. godine na kojem je predstavio deset problema, među kojima se našao i problem mogućnosti pronalaska računalnog algoritma koji će za svaku diofantsku jednadžbu s cjelobrojnim koeficijentima odlučiti ima li cjelobrojnih rješenja ili ne. Taj problem srodan je problemu pronalaska metode kojom bi se za svaku matematičku tvrdnju moglo ustanoviti je li istinita ili nije. Hilbert je bio uvjeren kako je odgovor na to pitanje: „da”.

Iako se pokazalo suprotno, nasljeđe Hilbertova sna su naši moderni računalni uređaji za koje je zaslužan Turing. Sva moderna računala potječu iz njegovih dizajna pa ga se opravdano smatra najbitnijim utemeljiteljem računalne znanosti. Do današnjeg dana najbolji računalni sustavi imaju u sebi ugrađen Turingov stroj. Međutim, njegova ideja potekla je iz razmišljanja o Hilbertovu pitanju je li matematika odlučiva, pa bismo na neki način mogli reći kako moderna računala zapravo potječu od paradoksa samoreferiranja i teorije skupova. Mnogi povijesni neodlučivi problemi (kao npr. hipoteza kontinuuma), ali i mnogi popularni neodlučivi problemi (Igra života, problem domina ...) mogu se svesti na problem zaustavljanja Turingovog stroja zbog čega taj problem smatramo izrazito važnim. Također, egzistencija neodlučivih problema znači da je moguće da se hipoteze poput Goldbachove[1] ili one da brojeva blizanaca ima beskonačno mnogo također mogu svesti na problem zaustavljanja pa možda nikada nećemo saznati odgovor na njih.

David Hilbert preminuo je 1943. godine. Na njegovom epitafu piše slogan iz znamenitog govora 1900.: „Moramo znati – znat ćemo”. Zapravo, nekada ne znamo, nekada nećemo ni moći saznati, ali pokušavajući saznati otkrivamo nove stvari koje mogu promijeniti svijet – kao što ga je rješavanje problema neodlučivosti promijenilo [25].

[1] Goldbachova pretpostavka kaže da je svaki paran prirodan zbroj dva prosta broja.

Bibliografija

[1] M. Balaguer, *Kurt Gödel*, Encyclopedia Britannica, 2022.

[2] J.T. Baldwin, O. Lessmann, *What is Russells' paradox?*, Scientific American (1998.)

[3] E.R. Berlekamp, J.H.Conway, R.K. Guy, *Winning Ways for your Mathe- matical Plays Vol. 4.*, A K Peters, Wellesley, 2004.

[4] A.P. Bird, *Logicism, Formalism, and Intuicionsm*, dostupno na `https://www.cantorsparadise.com/logicism-formalism-and-intuicionism-f5beeabcd375`, (travanj, 2022.)

[5] F.M. Brückler, *Povijest matematike*, PMF – Matematički odsjek, 2022.

[6] A. Churchill, S. Biderman, A. Herrick, *Magic: The Gathering is Turing Complete*, dostupno na `https://arxiv.org/abs/1904.09828v2`, (rujan, 2022.)

[7] M. Davis, *Hilbert's tenth problem is unsolvable*, The American Mathematical Monthly 80 (1973) 233-269

[8] M. Davis, *Logic and the development of the computer*, In: Handbook of the History of Logic Vol. 9. North-Holland, 2014, 31–38.

[9] J.W. Dawson, *Gödel and the limits of logic*, Plus Magazine, 2006.

[10] *Entscheidungsproblem*, dostupno na `https://hr.wikipedia.org/wiki/Entscheidungsproblem`, (travanj, 2022.)

[11] J. Eschenburg, *Sternstunden der Mathematik*, Springer Spektrum, 2017.

[12] S. Feferman, *Deciding the Undecidable: Wrestling with Hilbert's problems*, dostupno na `https://math.stanford.edu/~feferman/papers/deciding.pdf`, (kolovoz, 2022.)

[13] D. Hilbert, *Hilbertiana*, Wissenschaftliche Buchgesellschaft Darmstadt, 1964.

[14] *Hilbert's program*, dostupno na https://plato.stanford.edu/entries/hilbert-program/, (travanj, 2022.)

[15] *Hilbert's tenth problem*, dostupno na https://en.m.wikipedia.org/wiki/Hilbert%27s_tenth-\protect\@normalcr\relax_problem, (kolovoz, 2022.)

[16] A. Kids, *Richard's paradox*, dostupno na https://academickids.com/encyclopedia/index.php/Richard%27s_paradox, (rujan, 2022.)

[17] E. Jeandel, P. Vanier, *The Undecidability of the Domino Problem*, dostupno na https://www.lacl.fr/pvanier/rech/cirm.pdf, (travanj, 2022.)

[18] N. Johnston, *Lifeline is now online*, dostupno na http://www.nathanieljohnston.com/tag/conways-game-of-life/, (travanj, 2022.)

[19] D.E. Joyce, *Euclid's Elements – Book 1*, dostupno na http://aleph0.clarku.edu/~djoyce/elements/bookI/propI4.html, (rujan, 2022.)

[20] G. Kriesel, *Hilbert's programme*, Dialectica, 12(1958), 346–372

[21] L.B. Kuijer, *Solving the undecidability of the continuum hypothesis: a short summary of the results since 1963.*, dostupno na https://fse.studenttheses.ub.rug.nl/8400/1/Bouke_Kuijer_bachelor.pdf, (rujan, 2022.)

[22] E. Luft, *The Foundations of Mathematics: Hilbert's Formalism Vs. Brouwer's Intuitionism*, dostupno na https://www.encyclopedia.com/science/encyclopedias-almanacs-transcripts-and-maps/foundations-mathematics-hilberts-formalism-vs-brouwers-intuitionism, (travanj, 2022.)

[23] *Magic: The Gathering*, dostupno na https://en.m.wikipedia.org/wiki/Magic:_The_Gath-\protect\@normalcr\relaxering, (kolovoz, 2022.)

[24] V.W. Marek, J. Mycielski, *Foundations of Mathematics in the TwentiethCentury*, The American Mathematical Monthly 108 (2001), 449–468

[25] D. Muller, *Math has a Fatal Flaw*, dostupno na https://www.youtube.com/watch?v=HeQX2HjkcNo, (travanj, 2022.)

[26] J. Ouellette, *It's possible to build a Turing machine within Magic: The Gathering*, dostupno na https://arstechnica.com/science/2019/06/its-possible-to-build-a-turing-machine-within-magic-the-gathering/, (kolovoz, 2022.)

[27] P. Rendell, *This is a Turing Machine implemented in Conway's Game of Life*, dostupno na http://rendell-attic.org/gol/tm.htm, (rujan, 2022.)

[28] N. Saxena, *Hilberts Entscheidungsproblem, the 10th Problem and Turing Machines*, dostupno na https://www.cse.iitk.ac.in/users/nitin/talks/Oct2012-Turing.pdf, (rujan, 2022.)

[29] M. Segre, *Peano's Axioms in their Historical Context*, Archive for History of Exact Sciences, 48(1994), 201–342

[30] G. Shawcross, *Wang Tiles and Aperiodic Tiling*, dostupno na grahamshawcross.com/2012/10/12/wang-tiles-and-aperiodic-tiling/, (rujan, 2022.)

[31] V. Šego, *Turingovi strojevi*, dostupno na https://web.math.pmf.unizg.hr/nastava/gr/materijali-/v06/turingov_stroj-vjezbe.pdf, (rujan, 2022.)

[32] Z. Šikić, *Gödelovi teoremi*, Poučak, 2012.

[33] A. M. Turing, *On computable numbers, with an application to the Entscheidungsproblem*, Proceedings of the London Mathematical Society, Series 2h, 42 (1936), 230–265

[34] K. Wessen, *Not just a matter of time: The halting problem*, Plus Magazine, 2016.

[35] N. Wolchover, *How Gödel's proof works*, Quanta Magazine, 2020.

[36] T. Yuyama, *Undecidability of Hilbert's Tenth Problem and its Applications*, dostupno na http://t-yuyama.jp/pdfs/Undecidability-of-Hilberts-Tenth-Problem-and-its-Applications.pdf, (rujan, 2022.)

Sažetak

U ovom radu predstavljen je povijesno–popularni pregled problema (ne)odlučivosti. Krenuli smo od Cantorovog utemeljenja teorije skupova i postavljanja hipoteze kontinuuma. S obzirom da je još od Euklidovih „Elemenata" bilo opće prihvaćeno kako se provode (geometrijski) dokazi, teorija skupova izazvala je veliku raspravu o tome koja su sredstva dozvoljena u matematičkim dokazima. S jedne strane rasprave nalazili su se intuicionisti i konstruktivisti, a s druge formalisti. Najistaknutija osoba rasprave bila je David Hilbert, pa smo predstavili njegov znameniti govor o matematičkim problemima (od kojih je jedan, drugi bio upravo problem dokaza konzistentnosti Peanove aritmetike) te Hilbertov program – prijedlog za formalno utemeljenje i ujedinjenje matematike. Dio toga programa je i znameniti *Entscheidungsproblem*, pitanje postoji li algoritam koji bi za dani aksiomatski sustav i tvrdnju dao odgovor je li ta tvdnja dokaziva. Pokušavajući riješiti drugi Hilbertov problem, Kurt Gödel je dokazao znamenite teoreme o nepotpunosti kojima je pokazao neostvarivost Hilbertovog programa. Gotovo istovremeno Alan Turing koji se bavio s Hilbertovim *Entscheidungsproblem* i negativno ga riješio uvevši koncept stroja koji se naziva Turingov stroj iz kojeg su se razvila današnja računala. Naime, uspio je dokazati je da se ne postoji algoritam koji bi za dani program i pripadni ulaz odredio hoće li se program ikada zaustaviti ili neće (neodlučivost problema zaustavljanja). To otkriće bilo je izrazito bitno jer se mnogi drugi neodlučivi problemi mogu svesti na problem zaustavljanja. U drugom dijelu rada ukratko smo opisali četiri primjera neodlučivih problema kao što su: pitanje može li se za dvije dane konfiguracije u Igri života utvrditi hoće li druga ikad nastati iz prve; problem utvrđivanja može li se danim skupom Wangovih pločica popločati ravnina; Hilbertov deseti problem; problem optimalne strategije u igri *Magic: The Gathering*.

Summary

This thesis presents a historic and popular review of the problem of (un)decidability. We start with Cantor's foundation of set theory and his posing of the continuum hypothesis. Given that since Euclid's „Elements" the way of carrying out (geometric) proofs generally established the appearance of set theory caused a great debate about which means are allowed in mathematical proofs. On one side of the debate were intuitionists and constructivists, and on the other were formalists. The most prominent person in this debate was David Hilbert. We describe his famous speech about mathematical problems (the second of which was the problem of determining the consistency of Peano arithmetic), and Hilbert's programme – a proposal for the formal foundation and unification of mathematics. Trying to solve Hilbert's second problem, Kurt Gödel proved his famous incompleteness theorems, which implied that Hilbert's programme is not realisable. At the same time Alan Turing, was investigating Hilber's *Entscheidungsproblem*, and solved it negatively by introducing the concept of a machine called the Turing machine, the basis of all modern computers. Namely, he proved the undecidability of the halting problem: there does not exist an algorithm which could for any given programme and input determine if the programme will ever halt (i.e., the halting problem is undecidable). This discovery was extremely important because many other undecidable problems can be reduced to the halting problem. In the second part, we give a short description of four famous and provenly undecidable problems: the problem of determining if a given configuration will ever transform to another given configuration in the Game of Life; the problem of determinin if a given set of Wang tiles can tile the plane; Hilbert's tenth problem; the problem of optimal strategy in the game *Magic: The Gathering*.

Životopis

Rođena sam 11.02.1997. godine u Zagrebu, gdje sam i odrasla. Paralelno s osnovnom školom, završila sam i glazbenu školu; smjer: violina. 2011. godine upisala sam matematički smjer V. gimnazije u Zagrebu, a 2015. nastavnički smjer na Prirodoslovno–matematičkom fakultetu u Zagrebu, te sam 2020. stekla titulu sveučilišne prvostupnice edukacije matematike. Iste godine upisala sam diplomski studij matematike; smjer: nastavnički, također na Prirodoslovno–matematičkom fakultetu u Zagrebu, kojeg ću završiti obranom ovog rada.